ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2016

Volume XVII

PUBLICATION COURONNÉE PAR
L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

LES SYSTÈMES D'ARMEMENT LÉTAUX AUTONOMES ET LE *JUS AD BELLUM*

PAR

ELÉONORE GABRIEL (*)

L'objet de cette contribution est d'examiner les systèmes d'armement létaux autonomes (SALA) au regard du *jus ad bellum* ou droit international du maintien de la paix, c'est-à-dire au regard des dispositions relatives à l'interdiction de l'usage de la force dans les relations internationales.

Les SALA sont des systèmes robotisés fonctionnant sur la base de programmes informatiques, dotés de dispositifs létaux, et qui se caractérisent par leur capacité d'entreprendre des actions sans intervention humaine, autrement dit d'être autonomes (1).

L'autonomie est ici envisagée dans le sens d'une indépendance décisionnelle ou « comportementale ». Elle recouvre principalement des opérations de repérage, d'identification, de ciblage et, plus problématique, d'élimination d'une cible. Afin de mener à bien les opérations précédemment énoncées, le robot doit être en mesure d'évaluer, d'anticiper, d'acquérir et interpréter des données et de communiquer. En d'autres termes il doit pouvoir s'adapter aux situations en temps réel afin de prendre une décision et de réaliser l'action adéquate consécutive à celle-ci.

L'usage de la force fait l'objet d'une prohibition contenue dans la Charte des Nations Unies et la coutume. Le but de cette dernière, en garantissant l'intégrité territoriale et l'indépendance des Etats souverains de la communauté internationale, est de leur permettre d'établir des relations pacifiques. Cette prohibition fait cependant l'objet d'exceptions, dont la principale consiste en l'utilisation de la force par un Etat à des fins défensives : il s'agit de la légitime défense individuelle.

Au regard de la complexité et de l'autonomie des systèmes étudiés, il est possible de se demander si la délégation de « pouvoir » qu'ils permettent, c'est-à-dire le fait de laisser un système décider d'utiliser la force et de l'employer, n'entraîne pas de conséquences particulières dans l'application

(*) Doctorante au Centre de droit international de l'Université Paris Ouest (Nanterre–La Défense, France).

(1) Department of Defense, United States of America, *Unmanned Systems Integrated Roadmap FY2011-2036*, 2011, p. 43: « *autonomous systems are self-directed toward a goal in that they do not require outside control* [and] *can develop modified strategies for themselves by which they select their behavior. An autonomous system is self-directed by choosing the behavior it follows to reach a human-directed goal.* [It] *may even optimize behavior in a goal-directed manner in unforeseen situations* (i.e., *in a given situation, the autonomous system finds the optimal solution). The special feature of an autonomous system is its ability to be goal-directed in unpredictable situations* ». Le degré d'autonomie, central dans la qualification de ces armes, peut varier selon les modèles.

traditionnelle des dispositions du *jus ad bellum*. Pour le vérifier, cette analyse s'attachera donc aux deux notions phares que sont l'interdiction du recours à la force et la légitime défense individuelle.

L'emploi offensif des SALA : Un usage de la force qualifiable d'agression ?

La notion fondamentale et première du *jus ad bellum* est comprise dans l'interdiction coutumière, retranscrite par l'article 2§4 de la Charte de 1945 (2), de l'usage de la force. Concernant le contenu de cette interdiction, l'usage illicite de la force se « limite » à l'usage d'une force armée (3). Jurisprudence (4) et doctrine ont précisé ce terme comme « *l'utilisation de la force* [...] *physique, de type militaire ou autrement hostile* » (5). Il s'agit donc d'une force qui entraîne des conséquences physiques, c'est-à-dire des dommages matériels.

Les SALA sont définis comme étant « létaux », ce qui implique dès lors nécessairement qu'ils sont dotés de la capacité de tuer et de causer des dommages aux biens ou aux personnes. A titre d'exemple, le Super aEgis II est un système autonome robotisé auquel est adjointe une arme (6). Il permet ainsi d'obtenir les mêmes résultats que peuvent engendrer une arme classique aux mains d'un être humain.

Quand on analyse les caractéristiques des SALA, il ne fait pas de doute que leur emploi, hors de l'hypothèse des exceptions prévues par la Charte, constituerait un emploi de la force armée illicite. Les SALA semblent bien remplir le caractère « armé » d'une attaque, c'est-à-dire d'une attaque illicite et pouvant atteindre le niveau d'une agression (7), ouvrant la voie au déploiement de la légitime défense.

Cependant, l'autonomie dont bénéficient les SALA permet dans une certaine mesure de leur déléguer l'usage de la force armée. Sur ce point, l'acquisition des SALA par les Etats pourrait ponctuellement entraîner

(2) Art. 2§4 de la Charte des Nations Unies, 1945 : « *Les membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout Etat, soit de toute autre manière incompatible avec les buts des Nations Unies.* »

(3) Documents de la conférence des Nations Unies sur l'organisation internationale, vol. IV, 1945, pp. 720-721.

(4) L'interdiction de l'emploi de la force est à examiner à la lumière d'autres dispositions pertinentes de la Charte. En son article 51, cette dernière reconnaît le droit naturel de légitime défense, individuelle ou collective, en cas d'agression armée. *Cf.* CIJ, *Avis consultatif sur la licéité de la menace ou de l'emploi d'armes nucléaires*, 8 juil. 1996, *Rec. 1996*, p. 244, §38.

(5) Robert Kolb, *Ius contra bellum : le droit international relatif au maintien de la paix*, Helbing Lichtenhahn, Bâle, 2009 (2e éd.), pp. 246-247.

(6) DoDAAM Systems L.T.D., *Super aEgis II - The Best Mobile RCWS*, disponible sur le site Internet www.dodaam.com/eng/sub2/menu2_1_4.php.

(7) L'agression est définie par l'article 3 de la résolution 3314 de 1974 de l'Assemblée générale des Nations Unies comme « *l'emploi de la force armée par un Etat contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat, ou de toute autre manière incompatible avec la Charte des Nations Unies* », notamment, bien que non limitativement, comme « l'invasion ou l'attaque du territoire d'un Etat par les forces armées d'un autre Etat [...] *Le bombardement* [...] *L'attaque* [...] *contre les forces armées terrestres, navales ou aériennes, la marine ou l'aviation civile d'un autre Etat* ».

certaines conséquences dans l'hypothèse d'un dysfonctionnement. Plus généralement, elle pourrait s'inscrire dans le phénomène de la baisse du seuil du recours à la force par les Etats.

Interdiction de l'usage de la force et SALA : l'hypothèse du dysfonctionnement

Le dysfonctionnement est vu ici comme une anomalie fonctionnelle, qui peut prendre plusieurs formes : un trouble du fonctionnement normal du système, la désobéissance et la manipulation informatique.

Qu'il s'agisse du *Super aEgis II* (8), du *Mk15-Phalanx* (9) ou de l'*Iron Dome*, systèmes défensifs anti-aériens ou navals de type *Close In Weapon Systems* (CIWS), tous sont capables de repérer, d'identifier, de cibler et de détruire une cible de façon autonome. Or ces opérations, bien qu'accomplies de façon autonomes, sont régies par un programme qui détermine les décisions à prendre en face d'une situation concrète et les actions physiques à réaliser en application de l'option décisionnelle choisie par le robot. Dès lors, un certain risque provient de la distanciation aussi bien physique qu'intellectuelle entre les machines et leurs opérateurs.

En effet, il est possible d'imaginer que ce type de SALA puisse être sujet à un dysfonctionnement. L'éloignement géographique ainsi que la complexité logicielle du système affectera la capacité de l'opérateur ou du donneur d'ordre à empêcher ou du moins limiter les conséquences d'un dysfonctionnement du robot.

Il serait possible d'opposer à cette idée que ces systèmes faisant généralement l'objet d'un contrôle global, bien que distancié, par un opérateur, celui-ci n'aurait pas tant besoin d'être présent sur place que devant l'interface de communication établissant le lien avec le robot. Sur ce point cependant, il est également possible de soulever des réserves : il est peu probable que la personne qui communique avec le SALA soit capable de « réparer » en temps voulu l'erreur logicielle qui est à l'origine d'une attaque. Enfin, si l'origine de l'erreur est matérielle et nécessite une réparation sur l'objet en lui-même, l'éloignement vis-à-vis de la machine reste bel et bien problématique.

Autre scénario, plus futuriste, celui d'un SALA bénéficiant d'une autonomie logicielle « totale » ou « d'intelligence artificielle ». Le *Deep Learning,* la technique de l'imitation du réseau neuronal humain, promet

(8) DoDAAM Systems L.T.D., *op. cit.*

(9) United States Navy, *MK 15 – Phalanx Close In Weapons System*, Fact file, 15 nov. 2013, disponible sur le site Internet www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2 ; Human Rights Watch / International Human Rights Clinic / Human Rights Program at Harvard Law School, *Loosing Humanity: the Case Against Killer Robots*, nov. 2012, p. 17 : « [it is] *the only deployed close-in weapon system capable of autonomously performing its own search, detect, evaluation, track, engage and kill assessment functions* ».

des avancées considérables en termes d'autonomie décisionnelle (10). Dans cette hypothèse, la problématique qu'il faudra peut-être envisager sera celle de la désobéissance. Sans anthropomorphisme, l'intelligence artificielle peut faire craindre que la machine ne soit pas capable de nuancer son raisonnement en temps réel de la même manière qu'un être humain ou que son système de valeur la conduise à privilégier une action contraire à une directive humaine.

Dans la situation où un robot pleinement autonome, sans aucun contrôle extérieur sur place ou à distance, se verrait attribuer une opération, il pourrait agir de la manière qui lui paraît la plus adéquate, en privilégiant, par exemple, la réalisation d'une action prohibée et en outrepassant les ordres donnés, afin de mieux servir sa mission initiale ou d'un degré d'importance supérieur. Le Human-Robot Interaction Laboratory de la Tufs University cherche à développer ce principe de désobéissance, c'est-à-dire à intégrer dans l'architecture de contrôle du robot la capacité de rejeter une directive humaine. Cette désobéissance reste pour le moment programmée par l'homme et étudiée dans un cadre de stricte opportunité (11).

Enfin, ces systèmes sont toujours dépendants de la technologie informatique : ils fonctionnent sur la base de systèmes informatiques au service d'une architecture de contrôle (12) qui permet au robot de disposer d'une capacité décisionnelle plus ou moins complexe selon le type d'architecture (13). Ils sont donc, comme tout système informatique, de potentielles cibles d'attaques cybernétiques.

Les plus notoires sont l'opération « Orchad » (14) et le ver Stuxnet. La première a permis à un avion de l'armée israélienne de détruire un site nucléaire syrien et de s'enfuir sans encombre en leurrant le système de

(10) Un robot pourra être capable d'apprendre seul à partir de données collectées en temps réel, et peut-être à l'avenir sans avoir recours à un autre programme que celui qui lui permet d'apprendre : Gary Stix, « Machines that teach themselves », *Scientist American*, vol CCCXIII, n°6, déc. 2015, p. 38 : « *Deep-learning networks consist of layer on layer of connected computer processing units called artificial neurons, each of which performs a different operation on the input at hand – say, an image to be classified.* [...] *The deeper the network – the more layers – the higher the level of abstraction at which it can operate* ».

(11) Gordon Briggs / Matthias Scheutz, « 'Sorry, I can't do that': developing mechanisms to appropriately reject directives in human-robot interactions », Association for Advanced Artificial Intelligence Fall Symposium, 12-14 nov. 2015, disponible sur le site Internet hrilab.tufts.edu/publications/briggsscheutz15aaaifs.pdf.

(12) « *Cette complexité induit de nombreuses exigences, notamment sur l'informatique censée gérer le fonctionnement du robot et supporter ses capacités d'action, d'adaptation, de décision, etc., cette 'intelligence' que lui confère son contrôle. C'est donc de l'architecture logicielle de contrôle, c'est-à-dire la manière dont est conçu et développé le logiciel chargé du contrôle du robot, dont nous allons discuter dans cet article.* », peut-on lire *in* Robin Passama / David Andreu, « Architecture de contrôle pour la robotique – Approches et tendances – Paradigme de conception des architectures de contrôle », *Techniques ingénieur*, 10 sept. 2014, p. 1.

(13) « *Classiquement, un robot peut être décomposé en trois parties distinctes :* [...] *un ensemble de capteurs,* [...] *un ensemble d'actionneurs ;* [...] *entre ces deux extrémités de la chaîne de commande, une architecture de contrôle choisissant l'action (comportement) à mettre en œuvre, en fonction de l'objectif de la mission, de l'état courant du robot et de celui de son environnement. C'est donc au sein de l'architecture de contrôle que sont concentrées les capacités décisionnelles du robot* », *ibid*., p. 3.

(14) John Leyden, « Israël suspected of hacking Syrian air defences: did algorithms clear path for air raid? », *The Register*, 4 oct. 2007, disponible à l'adresse www.theregister.co.uk/2007/10/04/radar_hack_raid/ ; Sharon Weinberger, « How Israël spoofed Syria's air defense system », *Wired*, 10 avr. 2007, disponible à l'adresse www.wired.com/2007/10/how-israel-spoo.

défense aérien de l'armée syrienne. La seconde visait les centrifugeuses de la centrale de Natanz en Iran qui, en manipulant leur vitesse de rotation, les a détruites sans que les opérateurs ne s'en aperçoivent (15).

La rencontre de cette technologie létale autonome et de la manipulation informatique ne semble pas irréaliste, notamment dans le but de détourner les SALA de leur mission première. Des tentatives de prise de contrôle et de manipulation des systèmes en question sont sans doute à prévoir. Une cyberattaque sophistiquée à l'encontre d'un SALA d'une armée gouvernementale pourrait ainsi permettre à son auteur de prendre le contrôle de celui-ci et d'en user à l'encontre d'une population civile ou d'un Etat – cela, alors même que l'Etat propriétaire des SALA n'a aucune intention d'en faire l'usage. A titre d'illustration, un laboratoire de l'Université de Washington, afin de vérifier la sécurité d'un robot chirurgical, a lancé plusieurs cyberattaques de sévérité croissante à son encontre pour finalement réussir à en prendre le contrôle et le manipuler (16).

Une telle opération pourrait engendrer des conflits entre l'Etat attaqué et l'Etat considéré comme attaquant. Or l'identification des auteurs d'une cyberattaque peut être limitée dès lors que le cyberespace est le lieu privilégié pour masquer son identité, voire, elle aussi, la manipuler. Vis-à-vis du *jus ad bellum*, cela peut empêcher l'attribution de l'attaque à un Etat, essentiel pour l'exercice d'une défense légitime.

Dernière hypothèse liée au cyberespace : les potentialités de *jamming*, c'est-à-dire le fait de brouiller les signaux qui rattachent l'arme à l'opérateur. Si le contact entre un SALA et l'opérateur est rompu, il est difficile d'envisager la réaction d'un système autonome.

La technique de distanciation entre l'opérateur et le champ de bataille n'est pas nouvelle, mais elle peut, dans des cas de manipulation informatique, accentuer la perte du contrôle humain sur la machine.

D'un point de vue moins technique, les SALA pourront baisser le seuil à partir duquel les Etats utilisent la force armée, c'est-à-dire augmenter les situations où un Etat décide de recourir à celle-ci. Un tel phénomène implique la réduction de la portée de l'interdiction conventionnelle et coutumière.

(15) Caroline Cohn, « Will the U.S.-Iran cyber conflict escalate? », 8 août 2013, disponible sur le site Internet www.payvand.com/news/13/aug/1071.html ; David Albright / Paul Brannan / Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, Institute for Science and International Security, Washington, 15 fév. 2011.

(16) Jennifer Langston, « UW researchers hack a teleoperated surgical robot to reveal security flaws », *UW Today*, 7 mai 2015, disponible à l'adresse www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/.

Les SALA comme outil de facilitation du recours à la force armée

Dans le cadre du *jus ad bellum* les inquiétudes relatives aux SALA se concentrent sur l'escalade des conflits et l'éventualité d'une baisse du seuil du recours à la force.

D'une part, les SALA font craindre, comme cela a été constaté pour les drones, le rejet ou la réduction des proportions de chance d'une résolution pacifique des différends. Ici, c'est l'asymétrie des conflits qui est au cœur du problème. Les SALA sont pour le moment utilisés par des pays puissants et développés. S'ils sont employés à l'encontre d'êtres humains, c'est-à-dire à l'encontre d'un Etat qui ne disposerait pas d'une telle technologie, alors l'équilibre des forces est rompu de façon inéluctable. Le ressentiment certain causé par des pertes humaines en face de machines laisse peu de place à l'espoir du règlement prompt et pacifique d'un différend interétatique (17).

D'autre part, ne faut-il pas redouter que l'acquisition de tels systèmes par un grand nombre d'Etats les induise à recourir aux SALA dans des cas où ils se seraient refusé à déployer une force armée au moyen d'êtres humains, baissant ainsi le seuil du recours à la force ?

Sur ce point, la considération la plus évidente concerne l'intérêt stratégique des SALA, qui résulte de la réduction de pertes humaines qu'ils permettent et, dans une moindre mesure, de la réduction du coût de déploiement de ces machines en lieu et place d'êtres humains (18).

Enfin, en augmentant les capacités offensives des Etats, les SALA pourraient également s'inscrire dans la tendance, soutenue par une partie de la doctrine, à recourir à la force de façon préventive (19), baissant de cette autre manière le seuil du recours à la force armée et, en conséquence, générant une probable course à l'armement.

C'est la notion de légitime défense, consécutive à un emploi de la force illicite, qui sera à présent envisagée. Parmi les exceptions à l'interdiction du recours à la force, se pose en règle fondamentale le droit pour tout Etat qui se verrait agressé par un autre Etat de répondre par la force à son agresseur (20). En théorie, si l'usage de SALA est considéré comme

(17) Cette crainte a notamment été avancée par la délégation du Sri Lanka lors d'une réunion d'experts sur les SALA qui a eu lieu en avril dernier à l'Organisation des Nations Unies dans le cadre de la Convention sur certaines armes classiques. *Cf.* le site Internet www.unog.ch/80256EDD006B8954/%28httpAssets%29/30534E70A6CFAAC6C1257E26005F2B19/$file/2015_LAWS_MX_Sri+Lanka.pdf.

(18) Christof Heyns, *Rapport du Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires*, Conseil des droits de l'homme, Assemblée générale des Nations Unies, 23e session, 9 avr. 2013, A/HRC/23/47, p. 11, §58 : « *Due to the low or lowered human costs of armed conflict to States with LARs in their arsenals, the national public may over time become increasingly disengaged and leave the decision to use force as a largely financial or diplomatic question for the State, leading to the "normalization" of armed conflict LARs may thus lower the threshold for States for going to war or otherwise using lethal force, resulting in armed conflict no longer being a measure of last resort.* »

(19) Ce recours à la force est en réalité considéré par la doctrine qui la soutient comme un recours à la légitime défense. Il s'agit donc d'employer la force dans un but défensif et dans un temps préalable à la réalisation d'une agression.

(20) Charte des Nations Unies, art. 51.

un usage de la force armée, pouvant atteindre le niveau d'une agression armée, il permet à l'Etat agressé de recourir à la légitime défense.

L'exercice de la légitime défense individuelle suite a une agression au moyen de SALA

Au niveau de l'articulation entre l'agression et la défense légitime qu'elle permet de mettre en œuvre, les SALA peuvent poser deux types de difficultés. Dans le cas d'une agression suite à un dysfonctionnement évoqué plus haut ou encore au regard des acteurs qui les emploient.

Conséquences d'un dysfonctionnement vis-à-vis de la légitime défense

Il est tout d'abord nécessaire d'opérer une distinction en fonction du type de dysfonctionnement : s'il s'agit d'une erreur logicielle ou d'une « désobéissance ».

En premier lieu, dans le cas d'une anomalie fonctionnelle qui conduirait à un usage de la force illicite, c'est-à-dire dans le cas d'un usage de la force équivalent à une agression perpétrée par erreur, et dans la mesure où le SALA reste appréhendé par le droit comme un bien de l'Etat, il sera possible de se demander si l'Etat propriétaire du SALA pourrait se voir considéré comme un agresseur – ce qui ouvrirait l'exercice du droit à la légitime défense par l'Etat agressé – ou seulement voir sa responsabilité internationale engagée.

Ensuite, dans l'hypothèse où une attaque équivalant à une agression armée est perpétrée en désobéissance par un SALA qui fonctionne au moyen d'une intelligence artificielle aboutie, on peut se demander si ce dernier, au regard de l'étendue de ses capacités « intellectuelles », devra encore être considéré comme un simple bien de l'Etat qui le possède ou si on pourra le considérer comme un organe *de jure* ou *de facto* de l'Etat (21), ce qui permettrait d'attribuer l'agression à ce dernier selon les mêmes critères qu'en cas de désobéissance humaine.

Dès lors que l'intention n'est pas requise pour qualifier l'agression (22), l'Etat qui en agresserait un autre par erreur devrait pouvoir être la cible d'une défense armée légitime, ainsi que voir sa responsabilité engagée. Dans le même temps, si l'erreur était prise en considération dans une telle situation par le droit international, l'Etat qui se défend d'une agression

(21) Projet de la CDI sur la responsabilité de l'Etat, 2001, art. 4, 5 et 7.

(22) Jaroslav Zourek, « Définition de l'agression », *Recueil des cours de l'académie de La Haye*, vol. XCII, 1957, pp. 843-844 : « *L'erreur de fait comme l'erreur de droit est absolument inopérante dans ce domaine et ne peut ni exclure la légitime défense ni la responsabilité de l'Etat dont les forces ont commis l'attaque.* ». L'article 3 de la résolution 3 314 sur la définition de l'agression reste indifférent à la détermination de l'intention de l'agresseur, en énonçant notamment que les actes qualifiés d'agression le sont indépendamment du fait « *qu'il y ait eu ou non une déclaration de guerre* », indice de l'intention de l'Etat qui la déclare. Son article 2 précise en effet que « *l'emploi de la force armée en violation de la Charte par un Etat agissant le premier constitue la preuve suffisante à première vue d'un acte d'agression* ».

commise par erreur pourrait-il alors raisonnablement être considéré à son tour comme un agresseur ?

Dans la seconde hypothèse, celle d'une désobéissance, la question se place également sur le terrain de l'imputabilité de l'agression à un Etat. Au regard du droit international actuel, si le SALA qui désobéit – et agresse un Etat – est considéré comme un organe *de jure* ou *de facto* de l'Etat, alors la légitime défense devrait pouvoir être employée à l'encontre du premier Etat sans que son défaut d'implication ne soit pris en compte (23).

Le résultat reste donc inchangé, quel que soit le degré d'autonomie décisionnelle du robot. Ces solutions classiques semblent pourtant peu satisfaisantes concernant les situations étudiées en raison de ce fait nouveau : la délégation par l'Etat de la force létale, mais, surtout, de la décision d'y recourir, à une machine.

Sur le plan de la légitime défense, un autre écueil peut être alimenté par l'utilisation des SALA. Il s'agit de la tendance dans laquelle s'inscrira sans doute leur déploiement : la mise en œuvre d'une défense « légitime » suite à une attaque menée au moyen des SALA par des acteurs non étatiques.

La légitime défense à l'encontre d'acteurs non étatiques et l'agression au moyen de SALA

Le droit international du maintien de la paix reconnaît le droit dérogatoire des Etats d'user de la force dans le cas d'une agression préalable par un autre Etat. En effet, l'article 51 de la Charte des Nations Unies ne fait référence qu'aux cas d'agression, elle-même définie comme une attaque armée perpétrée par un Etat à l'encontre d'un autre.

Le *jus ad bellum* ne reconnaît pas aujourd'hui de « statut » aux acteurs non étatiques, excepté dans la mesure où ceux-ci sont rattachables à un Etat en fait ou en droit. Cependant, force est de constater qu'ils constituent une donnée non négligeable dans les conflits armés contemporains. Il existe une abondante littérature sur la perte des Etats du monopole de la force et sur l'apparition, dans ce domaine, d'acteurs privés qui sont difficilement, voire non rattachables à un Etat. Pour les SALA et comme cela était le cas par le passé, la question de savoir si le droit international autorise les Etats à utiliser la force en réponse à l'agression d'acteurs non étatiques n'est pas résolue.

L'article 2§4 de la Charte des Nations Unies envisage l'intervention armée sur le territoire d'un Etat comme un usage de la force prohibé. Dès lors, si l'attaque équivaut à une agression et en faisant une lecture stricte du contenu de la norme, le fait pour un Etat A, agressé par les SALA d'un groupe armé situé sur le territoire d'un Etat B, d'attaquer ces derniers en lançant une offensive sur le territoire de l'Etat B constitue une violation de l'intégrité territoriale de ce dernier et ainsi viole sa souveraineté.

(23) Au regard de l'article 7 du Projet de la CDI, la désobéissance ou l'excès de pouvoir d'un organe de l'Etat n'a pas d'effet sur l'attribution de la violation d'une obligation à cet Etat.

Les arguments opposés soutiennent que l'Etat B perd en quelque sorte son droit au respect de son intégrité territoriale en ne prenant pas les mesures nécessaires pour éviter les attaques perpétrées par les acteurs non étatiques en provenance de son territoire. Il manquerait ainsi à son obligation de *due diligence* et ouvrirait de ce fait la voie à l'exercice d'une légitime défense de l'Etat A qui pallierait à sa défaillance (24).

Concernant les SALA, il faut en premier lieu garder à l'esprit que la matière première est loin d'être inaccessible et qu'avec l'avènement de l'ère de l'*open source* (25) et de l'espionnage industriel, tout l'arsenal logiciel, requérant des connaissances scientifiques pointues, pourra sortir des laboratoires de recherche et des industries concernés. Reste la possibilité à ces acteurs d'acquérir des SALA auprès des fabricants, du marché noir, d'Etats sympathisants ou encore par le contrôle du territoire d'un Etat qui en possède. Dans tous les cas, ces nouvelles technologies seront sans doute très convoitées par les acteurs en question dès lors qu'elles leur éviteront de perdre des vies et d'agir à distance au moyen d'une puissance létale renforcée. L'hypothèse de SALA aux missions « suicide » semble, par exemple, assez probable.

(24) La Cour internationale de Justice (CIJ), quand elle en a eu l'occasion, n'a pas répondu à la question de savoir si l'usage de la force sur le territoire d'un Etat concentré sur les acteurs non étatiques – et non à l'encontre de l'Etat sur le territoire duquel ils se trouvent – était admis par le droit international du maintien de la paix. *Cf.* CIJ, *Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)*, 19 déc. 2005, *Rec. 2005*, p. 223, §146 : « *la Cour considère que les conditions de droit et de fait justifiant l'exercice d'un droit de légitime défense par l'Ouganda à l'encontre de la RDC n'étaient pas réunies.* [...] *elle n'a pas à se prononcer sur* [...] *la question de savoir si* [...] *le droit international contemporain prévoit un droit de légitime défense pour riposter à des attaques d'envergure menées par des forces irrégulières* ».

(25) Un chercheur américain a développé un algorithme de vision télescopique permettant à un drone d'éviter des obstacles à une vitesse de 50 km/h et a permis que son programme soit diffusé en *open source* : Computer Science and Artificial Intelligence Laboratory, « Self-flying drone dips, darts and dives through trees at 30 mph », 26 oct. 2015, disponible sur le site Internet www.csail.mit.edu/drone_flies_through_forest_at_30_mph. L'Open Source Robotics Foundation s'est joint à la DARPA pour faire la promotion du Robotics Fast Track Program, qui consiste à financer des projets en robotique afin de faire avancer plus rapidement la recherche. Ces financements sont proposés par la DARPA, elle-même financée par le Pentagone américain : *Robotics Fast Track Program, Overview*, disponible sur le site Internet rft.osrfoundation.org/index.html#overview.